WHAT IS CLAIMED IS:

1. A method of providing communications security, the method comprising:

(a) generating a protected content stream from a data stream;

(b) transmitting the protected content stream across a first short-range communications link; and

(c) transmitting across a second short-range communications link information for converting the protected content stream into the data stream.

2. The method of claim 1, wherein the protected content stream comprises a packet, and wherein step (a) comprises inserting one or more errors into the packet.

3. The method of claim 2, wherein step (a) further comprises inserting the one or more errors into a portion of the packet, the portion at a predetermined position within the packet.

4. The method of claim 3, wherein step (a) further comprises selecting the predetermined position.

5. The method of claim 3, wherein step (a) further comprises generating the one or more errors with a code.

6. The method of claim 5, wherein the code is based on a polynomial.

7. The method of claim 5, wherein step (c) comprises transmitting the predetermined position and the code across the second short-range communications link.

8. The method of claim 2, wherein the packet includes a field containing an error detection code and/or an error correction code, the method further comprising:

setting the error detection code and/or the error correction code after said inserting step.

9. The method of claim 8, wherein the error detection code and/or the error correction code includes a cyclical redundancy check (CRC) code.

10. The method of claim 1, wherein step (a) comprises:

formatting the data stream into a plurality of data packets, each the data packets including a field having an error detection code and/or error correction code;

generating at least one additional packet, the additional packet including a field having an error detection code and/or error correction code; and

arranging the at least one additional packet and the plurality of data packets into the protected content stream.

11. The method of claim 10, wherein the error detection codes and/or the error correction codes for the data packets and the at least one additional packet each include cyclical redundancy check (CRC) codes.

12. The method of claim 10, wherein step (a) further comprises randomly selecting a position of the at least one additional packet in the protected content stream.

13. The method of claim 10, wherein step (c) comprises transmitting across the second short-range communications link a position of the at least one additional packet in the protected content stream.

14. The method of claim 1, wherein step (a) comprises:

placing the data stream into a plurality of packets, each the packets including a field having an error correction code;

setting the error error correction code for each of the packets; and

injecting errors into one or more of the plurality of packets, such that the corresponding error correction codes are unable to correct these errors.

15. The method of claim 14, wherein the error correction code is a block code.

16. The method of claim 14, wherein step (a) further comprises randomly selecting a value and a location for each of the injected errors.

17. The method of claim 14, wherein step (c) comprises transmitting the value and the location for each of the injected errors across the second short-range communications link.

18. The method of claim 1:

wherein step (a) comprises encrypting the data stream with an encryption key; and

wherein step (c) comprises transmitting the encryption key across the second short-range communications link.

19. The method of claim 1:

wherein step (a) comprises encrypting the data stream with an encryption key; and

wherein step (c) comprises transmitting a decryption key across the second short-range communications link, the decryption key corresponding to the encryption key.

20. The method of claim 1, wherein the first short-range communications link is an ultra wideband (UWB) link.

21. The method of claim 1, wherein the second short-range communications link is a Bluetooth link.

22. A wireless communications device, comprising:

means for generating a protected content stream from a data stream;

means for transmitting the protected content stream across a first short-range communications link; and

means for transmitting across a second short-range communications link information for converting the protected content stream into the data stream.

23. A method of providing communications security, the method comprising:

(a) receiving a protected content stream from a first short-range communications link;

(b) receiving from a second short-range communications link information for converting the protected content stream into a data stream; and

(c) generating the data stream from the protected content stream.

24. The method of claim 23, wherein the protected content stream comprises a packet having one or more inserted errors, the one or more errors at one or more corresponding positions within the packet.

25. The method of claim 24, wherein step (b) comprises receiving the one or more positions and a code for removing the inserted errors from the packet.

26. The method of claim 25, wherein the code is based on a polynomial.

27. The method of claim 23, wherein the protected content stream comprises a plurality of data packets and at least one additional packet.

28. The method of claim 27, wherein step (b) comprises receiving a position of the at least one additional packet in the protected content stream.

29. The method of claim 28, wherein step (c) comprises removing the at least one additional packet from the protected content stream.

30. The method of claim 23, wherein the protected content stream in encrypted, and wherein step (b) comprises receiving a key for decrypting the protected content stream.

31. The method of claim 23, wherein the first short-range communications link is an ultra wideband (UWB) link.

32. The method of claim 23, wherein the second short-range communications link is a Bluetooth link.

33. A wireless communications device, comprising:

means for receiving a protected content stream from a first short-range communications link;

means for receiving from a second short-range communications link information for converting the protected content stream into a data stream; and

means for generating the data stream from the protected content stream.

34. A wireless communications device, comprising:

a controller adapted to generate a protected content stream from a data stream;

a first transceiver adapted to transmit the protected content stream across a first short-range communications link; and

a second transceiver adapted to transmit across a second short-range communications link information for converting the protected content stream into the data stream.

35. The wireless communications device of claim 34, wherein the first short-range communications link is an ultra wideband (UWB) link and the second short-range communications link is a Bluetooth link.

36. A wireless communications device, comprising:

a first transceiver adapted to receive a protected content stream from a first short-range communications link;

a second transceiver adapted to receive from a second short-range communications link information for converting the protected content stream into a data stream; and

a controller adapted to generate the data stream from the protected content stream.

37. The wireless communications device of claim 36, wherein the first short-range communications link is an ultra wideband (UWB) link and the second short-range communications link is a Bluetooth link.